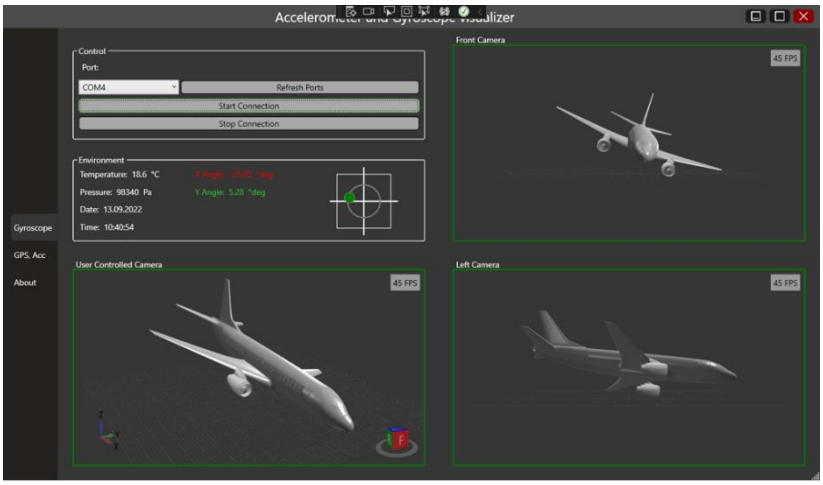


Рисунок 2 – Пример работы программного средства системы сбора информации с движущихся объектов

Список возможных применений подобной системы очень широк. Она может применятся для контроля грузов, перевозимых автомобильным и железнодорожным транспортом, для построения карт качества дорожных покрытий, для контроля технического состояния транспортных средств и много другое.

**Список использованных источников**

1. Авсяник, Е. С. Программно-аппаратный модуль мониторинга перемещения движущихся объектов / Е. С. Авсяник, Д. В. Деменковец // Веб-программирование и интернет-технологии WebConf 2021 : материалы 5-й Международной научно-практической конференции, Минск, 18–21 мая 2021 г. / Белорусский государственный университет ; редкол.: И. М. Галкин [и др.]. – Минск, 2021. – С. 57–58.

2. Авсяник, Е. С. Программно-аппаратное средство визуализации работы акселерометра и гироскопа / Авсяник Е. С., Мередов К., Деменковец Д. В. // Компьютерные системы и сети : сборник статей 58-й научной конференции аспирантов, магистрантов и студентов, Минск, 18–22 апреля 2022 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2022. – С. 62–64.

УДК 004.42

## ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ЭНТРОПИЙНОГО АНАЛИЗА ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

*Палуха В. Ю., Орлов А. А., Сергеев А. И.*
*НИИ прикладных проблем математики и информатики*
*e-mail: palukha@bsu.by*

***Summary.*** *We present description of the developed software, which realizes methods and algorithms of statistical analysis based on estimators of functionals of information entropy.*

**Энтропийный анализ.** Стойкость систем криптографической защиты информации зависит от того, насколько близка используемая ими случайная или псевдослучайная последовательность по своим свойствам к равномерно распределенной случайной последовательности (РРСП), что устанавливается с помощью статистических тестов. В них проверяется гипотеза $H_* = \{\{x_t\}$ является РРСП$\}\}$. В качестве тестовой статистики целесообразно

использовать статистические оценки энтропии. Пусть на вероятностном пространстве ($\Omega$, $F$, $P$) определена случайная величина $x$ из алфавита мощности $N = 2^s$ с дискретным распределением вероятностей $p = \{p_k\}, p_k = P\{x = \omega_k\}, p_k \geq 0, \sum_{k=1}^{N} p_k = 1, k = 1, \ldots, N$. В табл. 1 приведены формулы наиболее распространенных функционалов энтропии.

Таблица 1 – Функционалы энтропии

| | |
|---|---|
| Энтропия Шеннона | $H(p) = -\sum_{i=1}^{N} p_i \ln p_i$ |
| Энтропия Реньи | $H_2(p) = -\ln\left(\sum_{i=1}^{N} p_i^2\right)$ |
| Энтропия Тсаллиса | $S_2(p) = 1 - \sum_{i=1}^{N} p_i^2$ |

Пусть имеется реализация случайной последовательности $\{x_t : t = 1, \text{K}, n\}$ объема $n$. Рассмотрим асимптотику

$$n, N \to \infty, n/N \to \lambda, 0 < \lambda < \infty \tag{1}$$

и построим статистические оценки указанных функционалов энтропии. При построении оценок функционалов энтропии Реньи и Тсаллиса воспользуемся факториальными степенями $x^2 = x(x-1)$. При истинной гипотезе $H_*$ доказана асимптотическая нормальность и найдены асимптотические математическое ожидание и дисперсия в асимптотике (1): для оценки энтропии Шеннона в [1], для оценок энтропии Реньи и Тсаллиса – в [2].

Пусть $\alpha \in (0, 1)$ – заданный уровень значимости, $\hat{h}$ – статистическая оценка энтропии Шеннона, Реньи или Тсаллиса, $\mu_h$ и $\sigma_h^2$ – соответственно асимптотические математическое ожидание и дисперсия этих оценок. Решающее правило имеет вид [1, 2]:

$$\text{принимается} \begin{cases} H_*, & \text{если } t_- < \hat{h} < t_+; \\ \overline{H_*}, & \text{в противном случае,} \end{cases} \qquad t_\pm = \mu_h \pm \sigma_h \Phi^{-1}\left(1 - \frac{\alpha}{2}\right), \tag{2}$$

где $\Phi(\cdot)$ – функция распределения стандартного нормального закона.

Вычислим нормированную статистику

$$\hat{h}^0 = \frac{\hat{h} - \mu_h}{\sigma_h}. \tag{3}$$

Она в асимптотике (1) и при истинной гипотезе $H_*$ имеет стандартное нормальное распределение: $\hat{h}^0 : \mathcal{N}(0, 1)$. Следовательно, двустороннее $p$-значение для нее равно

$$p - value = 2\left(1 - \Phi\left(\left|\hat{h}^0\right|\right)\right). \tag{4}$$

Пусть наблюдается двоичная последовательность $\{y_\tau\}$, $\tau = 1, \ldots, T$. Из непересекающихся подряд идущих фрагментов длины $s$ ($s$-грамм) $X^{(t)} = (X_j^{(t)}) = = (y_{(t-1)s+1}, \text{K}, y_{ts}) \in \{0, 1\}^s$, $t = 1, \ldots, n = [T / s]$, сформируем новую последовательность $\{x_t\}$ из алфавита мощности $N = 2^s$

по правилу $x_t = \sum_{j=1}^{s} 2^{j-1} X_j^{(t)} + 1$. На основе критерия (2) вычислим последовательность нормированных отклонений оценки энтропии от математического ожидания в зависимости от $s$, которую назовем энтропийным профилем:

$$\chi(s) = \frac{\hat{h}(s) - \mu_h(s)}{\sigma_h(s)\Phi^{-1}(1-\alpha/2)} = \frac{\overline{h}(s)}{\Phi^{-1}(1-\alpha/2)}, \; s = s_-, \mathrm{K}\,, s_+. \qquad (5)$$

**Программный комплекс «ЭАДП»**

В НИИ ППМИ разработан программный комплекс «ЭАДП» [3], который позволяет применить критерий (2) к анализу двоичных файлов. В начале работы необходимо выбрать файл с последовательностью, порядок Big Endian или Little Endian, диапазон $s$ и функционалы энтропии. Вычисляемые значения добавляются на экран в режиме реального времени. Имеется возможность изменять уровень значимости α без пересчета оценок энтропии и переключаться на различные режимы отображения: непосредственно оценки энтропии $\hat{h}$, нормированные значения (5), $p$-значения (4). Помимо вывода самих значений в консоль, программа отображает графики зависимостей этих величин от длины фрагмента $s$. Главное окно программного комплекса с результатами работы представлено на рис. 1.

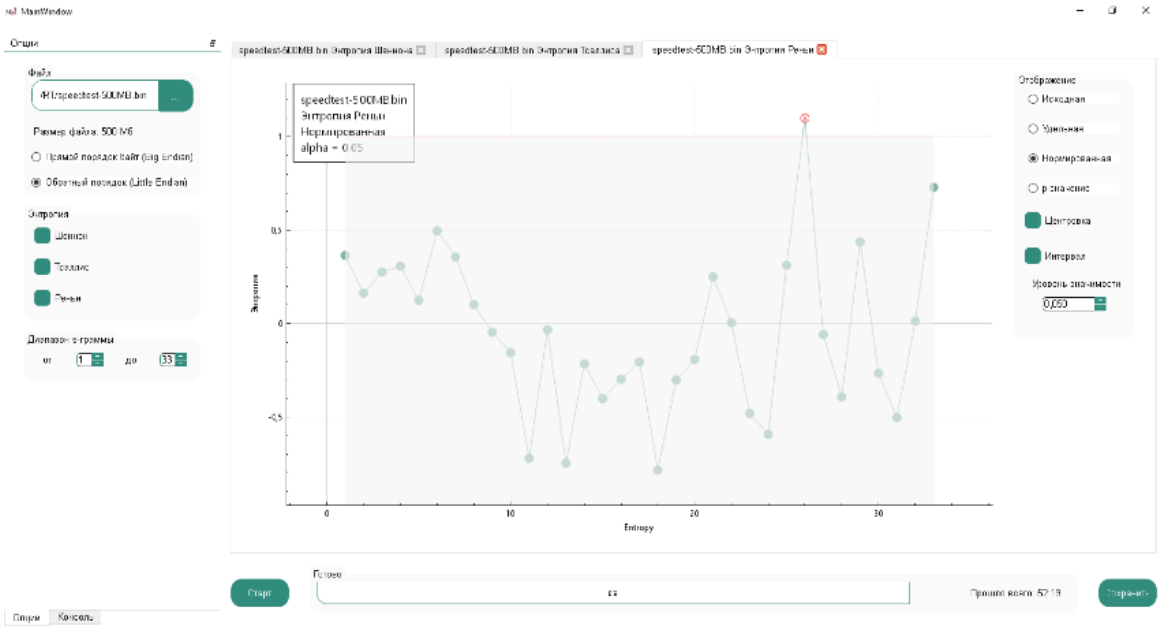


Рисунок 1 – Программный комплекс «ЭАДП»

**Список использованных источников**


1. Палуха, В. Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности / В. Ю. Палуха // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2017. – № 1. – С. 79–88.

2. Харин, Ю. С. Статистические оценки энтропии Реньи и Тсаллиса и их использование для проверки гипотез о «чистой случайности» / Ю. С. Харин, В. Ю. Палуха // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2016. – № 2. – С. 37–47.

3. Программное средство энтропийного анализа дискретных случайных последовательностей [Электронный ресурс]. – Режим доступа: http://www.product.bsu.by/katalog/ informacionnie-tehnologii/informacionnie-naukoemkie-tehnologii/statistika/programmnoe-sredstvo-entropijnogo-analiza-diskretnih-sluchajnih-posledovatel_nostej/. – Дата доступа: 19.10.2022